UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/036,333	12/24/2001	William D. Slyva	EMC01-41(00024)	3305

7590 03/17/2006

Barry W. Chapin, Esq.
CHAPIN & HUANG, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, MA 01581

EXAMINER	
HERRING, VIRGIL A	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/036,333	SLYVA ET AL.	
	Examiner	Art Unit	
	Virgil Herring	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-19,21-29,31-41,43-47,49-53,55-57,59 and 60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-19,21-29,31-41,43-47,49-53,55-57,59 and 60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is responsive to the amendment filed December 20, 2005. Claims 1-5, 7-19, 21-29, 31-41, 43-47, 49-53, 55-57, and 59-60 are pending. Claims 6, 20, 30, 42, 48, 54, and 58 are cancelled.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Specification

The amendment to the application filed on 12/20/05 does not comply with the requirements of 37 CFR 1.121(c) because a marked-up copy indicating the changes to the specification and claims was not provided. Amendments to the claims filed on or after July 30, 2003 must comply with 37 CFR 1.121(c) which states:

(c) *Claims.* Amendments to a claim must be made by rewriting the entire claim with all changes (*e.g.*, additions and deletions) as indicated in this subsection, except when the claim is being canceled. Each amendment document that includes a change to an existing claim, cancellation of an existing claim or addition of a new claim, must include a complete listing of all claims ever presented, including the text of all pending and withdrawn claims, in the application. The claim listing, including the text of the claims, in the amendment document will serve to replace all prior versions of the claims, in the application. In the claim listing, the status of every claim must be indicated after its claim number by using one of the following identifiers in a parenthetical expression: (Original), (Currently amended), (Canceled), (Withdrawn), (Previously presented), (New), and (Not entered).

(1) *Claim listing.* All of the claims presented in a claim listing shall be presented in ascending numerical order. Consecutive claims having the same status of "canceled" or "not entered" may be aggregated into one statement (*e.g.*, Claims 1–5 (canceled)). The claim listing shall commence on a separate sheet of the amendment document and the sheet(s) that contain the text of any part of the claims shall not contain any other part of the amendment.

(2) *When claim text with markings is required.* All claims being currently amended in an amendment paper shall be presented in the claim listing, indicate a status of "currently amended," and be submitted with markings to indicate the changes that have been made relative to the immediate prior version of the claims. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived. Only claims having the status of "currently amended," or "withdrawn" if also being amended, shall include markings. If a withdrawn claim is currently amended, its status in the claim listing may be identified as "withdrawn—currently amended."

(3) *When claim text in clean version is required.* The text of all pending claims not being currently amended shall be presented in the claim listing in clean version, *i.e.*, without any markings in the presentation of text. The presentation of a clean version of any claim having the status of "original," "withdrawn" or "previously presented" will constitute an assertion that it has not been changed relative to the immediate prior version, except to omit markings that may have been present in the immediate prior version of the claims of the status of "withdrawn" or "previously presented." Any claim added by amendment must be indicated with the status of "new" and presented in clean version, *i.e.*, without any underlining.

(4) *When claim text shall not be presented; canceling a claim.*

(i) No claim text shall be presented for any claim in the claim listing with the status of "canceled" or "not entered."

(ii) Cancellation of a claim shall be effected by an instruction to cancel a particular claim number. Identifying the status of a claim in the claim listing as "canceled" will constitute an instruction to cancel the claim.

(5) *Reinstatement of previously canceled claim.* A claim which was previously canceled may be reinstated only by adding the claim as a "new" claim with a new claim number.

Response to Arguments

With regards to the amendments to the specification, the examiner notes that a plethora of misspellings and extra words are still present, despite the previous objection.

With regards to applicant's response to the claim objections, the examiner notes that applicant asserts changes in claims 1, 6, and 30. The examiner can find no evidence that any change was actually made to overcome the objection to claim 1. Although claims 6 and 30 were cancelled, the points objected to (specifically, "first packet first packet communications sessions") were copied directly into claims 1 and 25 rather than being fixed to overcome the objections.

With regards to the rejection of claims 29, 33, and 34 under 35 USC § 101 and 112, the amendments are sufficient to overcome the previous rejections.

With regards to the rejection of claims 16, 40, 52, and 56 under 35 USC § 112, the amendments are sufficient to overcome the previous rejections.

Applicant's arguments filed on 12/20/05 have been fully considered but they are not persuasive. As explained below, the cited patent (Wookey, US Patent # 6,023,507) discloses all features of the claimed invention.

Applicant argued that Wookey does not disclose or suggest determining if the user of the computer system is authorized to establish the first packet communications system. Examiner respectfully disagrees. In column 9, lines 41-43, Wookey states that "the modem at the customer is password protected and the password is provided by the service center." It is well established in the computer security art that providing a

password is a method of verifying authorization to perform a task, the task in this case being establishing a packet communications session from the service center to a customer's modem.

Applicant then argued that since Wookey does not disclose determining if the user is authorized to establish the first packet communications session, he consequently fails to disclose allowing the computer system to perform the step of establishing a second packet communications session from the data communications device to a data storage system when the determination is that the user is authorized. Examiner respectfully disagrees. As shown above, Wookey does disclose determining if the user is authorized to establish the first packet communications session from the service center to the customer modem. The inherent next step would be to establish a packet communications session from the customer modem to the monitored customer computer system if and only if the service center provided the correct password to the customer modem.

Applicant then argued that Wookey also fails to disclose the step of denying the ability of the computer system to perform the step of establishing a second packet communications session from the data communications device to the data storage system when the determination is that the user is not authorized. Examiner respectfully disagrees. Because the purpose of providing a password is to provide proof that a user is allowed to perform some action, an incorrect password results in the denial of the

ability to perform that action. Since the password in Wookey is provided to a modem, the action in Wookey would be to establish a packet communications session. Thus, providing an incorrect password would prevent establishment of a packet communications session.

Claim Objections

Claim 1 is objected to because of the following informalities: lines 1-2 recite "a method for establishing a packet communication sessions". Revision to provide correct article/noun agreement is requested. Additionally, in lines 17-18 and 21-22, the limitation "the first packet first packet communications session" is recited. Deletion of the extraneous words is requested.

Claim 25 is objected to because of the following informalities: in lines 4 and 7-8 of page 82, the limitation "the first packet first packet communications session" is recited. Deletion of the extraneous words is requested. Appropriate correction is required.

Claim 29 is objected to because of the following informalities: in line 1, a pair of brackets is included, which suggests a deletion, but no text is located inside the brackets.

Claim 41 is objected to because of the following informalities: no period.

Claim Rejections - 35 USC § 101 & 112

A broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. See MPEP § 2173.05(c). Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10 USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" and then narrow language. The Board stated that this can render a claim indefinite by raising a question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949).

In the present instance, claims 1 and 25 recite the broad recitation “establishing a second packet communications session from the data communications device to a service processor associated with the data storage system”, and the claims also recite “if the user of the computer system is authorized to establish the first packet first packet communications session, allowing the computer system to perform the step of establishing a second packet communications session from the data communications

device to the data storage system; and if the user of the computer system is not authorized to establish the first packet first packet communications session, denying the ability of the computer system to perform the step of establishing a second packet communications session from the data communications device to the data storage system" which is the narrower statement of the range/limitation. Claims 1 and 25 are thus considered to be unclear, because the applicant first claims that the session is *conditionally* established, then claims that the session is *always* established, thus negating the step of authorizing the user to establish the second packet communications session.

Claim 59 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim preamble indicates that it is a system, but the claim from which it depends (claim 18) is a method, and thus claim 59 overlaps the two statutory classes.

Claim 59 is also rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter from a single statutory class which the applicant regards as the invention. The addition of method wording to a claim dependent on a system renders the claim language indefinite.

Claim Rejections - 35 USC § 102

Claims 1-5, 7-19, 21-29, 31-41, 43-47, 49-53, 55-57, and 59-60 are rejected under 35 U.S.C. 102(b) as being anticipated by Wookey (US Patent # 6,023,507).

With regards to claims 1, 25, 47, 49, and 56, Wookey discloses in a computer system, a method for establishing a packet communication sessions to a data storage system, the method comprising the steps of:

receiving a request to establish a communications session with a data storage system; (Col. 1, Lines 37-38: "the user of that computer system calls the remote service center.")

establishing a first packet communications session from the computer system to a data communications device capable of communicating with the data storage system, the establishing a first packet communications session comprising:

obtaining connection information for a data communications device that is capable of communicating with the data storage system; (Col. 9, Lines 4-5; If communications are always initiated from the service center, the service center must have the connection information for a data communications device stored somewhere on-site)

initiating the first packet communications session from the computer system to a data communications device using the connection information for the data communications device; (Col. 9, Lines 4-5)

providing, to the data communications device, first packet communications session authentication information such that the data communications device can determine if a user of the computer system is authorized to establish the first packet communications session, and (Col. 9, Lines 41-43)

if the user of the computer system is authorized to establish the first packet first packet communications session, allowing the computer system to perform the step of establishing a second packet communications session from the data communications device to the data storage system; and (Col. 9, Lines 41-43; If the password for the customer modem is accepted, it will open the second connection from the modem to the customer's monitored system)

if the user of the computer system is not authorized to establish the first packet first packet communications session, denying the ability of the computer system to perform the step of establishing a second packet communications session from the data communications device to the data storage system; (Col. 9, Lines 41-43; Conversely, if the password for the customer modem is not accepted, the second connection from the modem to the customer's monitored system would not be opened)

establishing a second packet communications session from the data communications device to a service processor associated with the data storage system; (Col. 9, Lines 41-43; The service center first negotiates the connection

with the customer modem before a connection between the modem and the monitored system is established)

and

performing packet communications between the computer system and the service processor associated with the data storage system using the first and second packet communications sessions. (Inherent; The communications connection between the service center and monitored system would be non-functional if packet communications were not performed)

With respect to claims 2 and 26, Wookey (507) discloses the method of claim 1 or 25 wherein the step of receiving a request to establish a communications session with a data storage system comprise the steps of:

receiving user authentication for a user of the computer system;

authenticating an identity of the user based on the user authentication information;

receiving a data storage system identity indicating an identity of the data storage system to which the packet communications session is to be established.

In column 8, lines 42-45 Wookey (507) states that "It is possible to protect each monitor with a unique password so that only authorized administrative personnel can access a given monitor for modification." Wookey (507) discloses a system for remotely

servicing multiple computer systems in which service personnel can receive information on which systems need service and then securely connect using established authentication techniques.

With respect to claims 3 and 27, Wookey (507) discloses the method of claim 2 or 26 wherein:

the request to establish a communications session with a data storage system includes the identity of the data storage system to which a communications session is to be established; and

wherein the identity specifies at least one of:

i) a phone number of a service processor modem associated with the data storage system; (Col. 9, Lines 40-45)

ii) a serial number of the data storage system; and (Col. 4, Lines 63-68)

iii) customer information related to a customer operating the data storage system. (Col. 4, Lines 63-68)

With respect to claims 4 and 28, Wookey (507) discloses the method of claim 2 or 26 wherein the step of receiving data storage system identity information comprises the steps of:

receiving data storage system search criteria;

providing data storage system search criteria to a connection monitor computer system to produce a set of data storage system identities that meet the data storage system search criteria; and

receiving the set of data storage system identities that meet the data storage system search criteria; and

allowing the user to select at least one data storage system identity from the set of data storage system identities.

Wookey (507) discloses that at startup, administration software searches for all monitor software on the same subnet (Col. 13, Lines 13-20). Thus, the criterion of the search is simply "all computers connected to this computer." This criterion is received from the administrator program code when the process begins to execute. The administrator software then displays a list of the accessible computers available for servicing, so that the user can select one to connect with (Fig. 8).

With respect to claims 5 and 29, Wookey (507) discloses the method of claim 4 or 28 wherein:

the data storage system search criteria is received from at least one of:

i) a user of the computer system;

ii) a service ticket identifying a data storage system;

the data storage system search criteria includes at least a portion of the user authentication information; and

the set of data storage system identities that meet the data storage system search criteria includes identities of data storage systems to which a user identified by the portion of the user authentication information is allowed to establish a packet communications session.

Since the invention of Wookey (507) searches for all connected computers when the administrator software starts running, one can say that the user supplies the search criteria by selecting which computers are on the same subnet as the computer running the administrator program (Col. 13, Lines 13-20). It is implicit that a program to inform the user of errors in the connected computers will apprise the user of any errors discovered (in other words, presenting a service ticket to the user). Wookey (507) discloses, in lines 50-54 of column 10, that the diagnostic data of the connected computers is password protected so that nobody other than a qualified service center engineer can access the information. Thus, since the search criteria are determined by physical connections (hard-wired) to the service computer, and access to the service computer is restricted by an authentication control subsystem, it is possible to state that the user authentication is a part of the search criteria because the user authentication is a component of one of the computers in the network which defines the search criteria.

With respect to claims 7 and 31, Wookey (507) discloses the method of claim 1 or 25 wherein the step of obtaining connection information for the data communications device comprises the steps of:

providing, to a connection monitor computer system, a request for an address of a data communications device, the request including data communications device selection criteria allowing the connection monitor computer system to select and return an address of an available data communications device that is authorized to establish the second packet communications session to the data storage system; and (Col. 4, Lines 47-53)

receiving the address of the data communications device selected by the connection monitor computer system. (Col. 4, Lines 47-53)

Wookey (507) discloses one modem (data communications device) for each small network of customer computer systems. Column 9, lines 40-41 indicate that the computer at the service center stores customer modem connection information in its internal memory. In this situation, a request for the address of the data communications device would take the form of a command to read from the hard drive or RAM.

With respect to claims 8 and 32, Wookey (507) discloses the method of claim 7 or 31 wherein the request for an address of the data communications device includes at least one of:

i) a portion of the user authentication information; (Col. 8, Lines 42-45)

ii) customer information concerning a customer operating the data storage system; and (Col. 4, Lines 62-65)

iii) connection information associated with the data storage system; and (Col. 4, Lines 62-65)

wherein the connection monitor computer system compares the request for an address against user and customer data to determine what data storage systems a user providing the request is allowed to access. (Col. 8, Lines 42-45)

Wookey (507) explains in column 8 that "it is possible to protect each monitor with a unique password so that only authorized administrative personnel can access a given monitor for modification." Protection with a unique password implies the use of user authentication information. Additionally, connection information associated with the system to which the user is attempting to connect would be inherently required. It is known to those in the art that connection authorization will involve comparing user data with data associated with the remote system. In this case, that would mean comparing the administrator's user data with the customer's information to determine if the administrator is authorized to modify that customer's monitor.

With respect to claims 9 and 33, Wookey (507) discloses the method of claim 1 or 25 wherein:

the step of initiating the first packet communications session establishes an internet protocol communications session between the computer system and the data communications device; and (Col.4 , Lines 47-50)

wherein the step of providing, to the data communications device, first packet communications session authentication information passes user authentication information from the computer system to the data communications device to allow the data communications device to authorize the internet protocol communications session. (Col. 8, Lines 42-45)

In column 4, Wookey (507) discloses that the modems of the vendor's modem pool are configured to connect to modems of the customer's monitored systems, and that the connection is under the control of a network terminal server. Thus, he has a communications session between a computer system and a data communications device. Since another connection between the data communications device and the monitored system exists implicitly, the connection from the vendor computer system to the data communications device can be described as the first packet communications session. Similarly, the connection from the data communications device is the second packet communications session. In column 8, Wookey (507) discloses the protection of the monitored computer systems using a unique password. A password implies authentication of the user at some point in the connection setup process. Authenticating the user to the remote network's server (the data communications device) is a well-known step in internet protocol communications.

With respect to claims 10 and 34, Wookey (507) discloses the method of claim 9 wherein the step of providing, to the data communications device, first packet

communications session authentication information causes the data communications device to communicate with a user account computer system to verify if the user of the computer system identified in the user authentication information is authorized to cause the data communications device to establish the first and second packet communications sessions from the computer system, through the data communications device, to the data storage system. (Col. 8, Lines 42-45)

Because the data communications device is a router or modem, a list of valid users would have to be stored elsewhere, because routers and modems have very little internal memory, which is used only to store the device's firmware and a list of valid IP addresses, or conversely, a list of blocked IP addresses. Thus, a separate computer system, which contains a list of valid users and their passwords, must exist inherently, and the data communications device must be able to communicate with it.

With respect to claims 11, 35, and 50, Wookey (507) discloses the method of claim 1 or 25 or 47 wherein the step of establishing a second packet communications session from the data communications device to the data storage system comprises the steps of:

providing, to the data communications device, second packet communications session connection information allowing the data communications device to initiate the second packet communications

session from the data communications device to the data storage system;

(Col. 4, Lines 47-50)

receiving second packet communications session state information indicating a state of the second packet communication session between the data communications device and the data storage system.

(Col. 9, Lines 52-65)

In column 4, Wookey (507) discloses the connection of the vendor modem to a customer modem under the control of a network terminal server. This clearly shows a first packet communications session from the vendor modem to the server, and a second packet communications session from the server to the customer modem. In this case, the network terminal server is acting as a router (data communications device). Those skilled in the art will recognize that in order to establish the connection between the router and the customer computer the user wishes to access, the router must be provided session information indicating to which computer the connection should be made. Column 9 shows the login and verification process for the connection. It is inherent that if verification is being carried out, then all parties involved in the verification are aware of it. Thus, at some point the data communications device must have received second packet communications session state information, which it would pass on to the vendor computer.

With regards to claims 12 and 36, Wookey (507) discloses the method of claim 11 or 35 wherein:

the second packet communications session connection information includes data storage system connection information associated with the data storage system and user authentication information of the user of the computer system; and (Col. 9, Lines 52-55)

wherein the step of providing the second packet communications session connection information to the data communications device causes the data communications device to perform the steps of:

initiating the second packet communications session from the data communications device to the data storage system using the data storage system connection information; (Col. 9, Lines 52-55)

providing the user authentication information to a remote access server associated with the data storage system to allow the remote access server to authorize the establishment of the second packet communications session from the data communications device to the data storage system; (Col. 8, Lines 42-48)

receiving data storage system address information at the data communications device identifying an address of the data storage system to allow the data communications device to establish the second packet communications session; and (Col. 9, lines 52-55)

> forwarding second packet communications session state information to the computer system from the data communications device to allow the computer system to perform packet communications between the computer system and data storage system using the first and second packet communications sessions. (Col. 9, Lines 52-55)

It is inherent to the system that the second packet communications session, between a router and the customer computer, must contain connection information for the customer computer. If it did not, the router would not know to which computer the user wishes to connect. Additionally, the inclusion of the user authentication information would be inherent, because without that information the customer computer would not know if the person attempting to establish a connection is a valid administrator. The steps listed in the connection procedure are also inherent requirements. Initiating the second packet communications session is inherent because that was the whole purpose of the connection process. Providing the user authentication information to a remote access server associated with the data storage system is inherent because that is the reason for having the user authentication information. Were it not provided to a server tasked to verification of remote users, then the data storage system would have no way of knowing if the user information is valid. The data communications device must inherently receive data storage system address information so that it can be sure that the correct connection was made. Finally, forwarding the second packet communications session state information to the vendor's computer system is inherent

because if the state information were not forwarded, the vendor's computer system would have no way of knowing if the connection to the data storage system was successful.

With respect to claims 13, 37, and 51, Wookey (507) discloses the method of claim 12 or 36 or 50 wherein the data storage system address information is a pre-configured network address assigned to the service processor associated with the data storage system.

Though it is never named as such, Wookey (507) inherently discloses the data storage system address information. It is known to those in the art that any computer system on a network or the Internet will always have an IP address or a modem phone number, which is the address of the computer on the network.

With regards to claims 14 and 38, Wookey (507) discloses the method of claim 12 or 36 wherein:

> the second packet communications session connection information includes data storage system connection information including a phone number of a service processor modem associated with the service processor associated with the data storage system; and (Col. 4, Lines 46-68)
>
> wherein the step of initiating the second packet communications session from the data communications device to the data storage system causes the data communications device to instruct a modem to dial the phone number of a

service processor modem in order to establish a dial up connection to the data storage system from the data communications device. (Col. 4, Lines 47-49)

Wookey (507) discloses a dialup connection between the vendor's computer system and a monitoring computer connected to one or more monitored systems. It is known to those in the art that in the process of communicating between the vendor's computer and the monitoring computer, packet communication sessions are established between the vendor computer, a router (data communications device) and the monitoring computer. If the vendor's modem is to dial the customer's modem, the phone number of the customer's modem is an inherent part of the information which must be transferred.

With respect to claims 15 and 39, Wookey (507) discloses the method of claim 12 or 36 wherein:

the second packet communications session state information includes the data storage system address information and includes data storage system connection bandwidth information; and

wherein the step of forwarding second packet communications session state information to the computer system from the data communications device causes the data communications device to perform the step of:

forwarding the second packet communications session state information to a network manager computer system which receives the second packet

communications session state information and forwards routing information to the computer system so that the computer system can perform packet communications with the data storage system. (Col. 4, Lines 49-52)

It is known to those in the art that communications session information is passed between two computers that are attempting to communicate with each other. This state information includes the address information for all involved computers, as well as connection speed information (bandwidth). If this information is not provided the computers will not have the knowledge necessary to communicate correctly. Wookey (507) discloses a connectivity server 304 that manages connections to the modem pool 301 inside the service center 101. One skilled in the art would recognize that a server that provides links to a modem pool would receive communications session information before finalizing the link between the vendor's computer and the service center modem pool.

With respect to claims 16, 40, and 52, Wookey (507) discloses the method of claim 12, 35, or 47 wherein the step performing packet communications between the computer system and the service processor associated with the data storage system comprises the steps of:

receiving the second packet communications session state information in response to the step of forwarding;

adjusting connection bandwidth associated with the first packet communications session to match connection bandwidth associated with the second packet communications session;

providing computer system address information to the data storage system so that the data storage system can establish a route to the computer system; and

using the first packet communications session between the computer system and the data communications device and the second packet communications session between the data communications device and the service processor associated with the data storage system to perform packet communications between the computer system and the service processor associated with the data storage system.

Though Wookey (507) does not go into great detail describing the connection process, he does disclose that the connection is secure and authenticated. From this knowledge, one skilled in the art would recognize that communications session state information would be available to all the communicating parties. This information typically includes such data items as the addresses of the computers and the connection bandwidth. It is inherent that the bandwidth must be adjusted to a uniform rate to prevent lost packets. If one computer is sending packets faster than the other computer is prepared to receive them, the information is simply lost. It is also inherent that since all the computers involved in the communications need to know the

addresses of the other computers, providing the computer system address information to the data storage system is a necessity. Finally, it is inherent that after all the time taken to set up a secure communications channel, that the channel would be used to perform packet communications between the computer system and the service processor associated with the data storage system.

With respect to claim 17, Wookey (507) discloses the method of claim 1 wherein the step of receiving a request to initiate a communications session with the data storage system further comprises the steps of:

receiving a service ticket from the data storage system; and (Col. 3, Lines 40-45)

analyzing the service ticket to determine an identity of the data storage system to which a packet communications session is to be established from the computer system. (Col. 3, Lines 62-67; Col. 4, Lines 1-3)

Wookey (507) discloses how the customer systems periodically perform a variety of diagnostic tests and transmit the results to the remote service center. Though he does not use the phrase "service ticket," the functionality is the same. It is well known to those in the computing art that data transmitted from one computer to another (such as a service ticket) will contain information regarding the origin of the data. Because Wookey (507) discloses a database of customer information, including the history of "diagnostic tests and patches that exist for a particular product" (Col. 4, Lines 66-67), the diagnostic information must be associated in the database to whatever customer system generated the information. Thus, it is inherent that any diagnostic information

transmitted to the service center can be analyzed to determine its origin. Since this information includes "error messages from log files, system crash data" etc. (Col. 3, Lines 63-64), the staff at the service center will know when to initiate communications to the customer system.

With respect to claim 18, Wookey (507) discloses the method of claim 1 wherein the steps of establishing a first packet communications session, establishing a second packet communications session, and performing packet communications are performed using secure and authenticated communications sessions. (Col. 10, Lines 55-60)

With respect to claims 19, 41, and 53, Wookey (507) discloses, in a processor in a data storage system a method for establishing a packet communications session with a computer system, the method comprising the steps of:

receiving a request to initiate a packet communications session, the request to initiate a packet communications session includes user authentication information of a user of the computer system; (Col. 1, Lines 37-40; Col. 9, Lines 5-7)

providing data storage system address information to an initiator of the request;

receiving computer system address information to allow the processor in the data storage system to perform packet communications with the computer system;

establishing a packet communications session with the computer system based on the computer system address information; and (Col. 1, Lines 40-42)

authenticating an identity of the user based on the user authentication information in order to authorize the establishment of the packet communications session to the data storage system. (Col. 8, Lines 42-45)

Wookey (507) describes how a remote support engineer will initiate a dial-up connection to a computer to perform analysis and maintenance. Those skilled in the art will recognize that dial-up connections, like other Internet connections, are inherently packet-based. Because connection information (such as an IP address, modem phone number, and connection bandwidth) is required for packet communications, it is inherent that at some point the monitored site provides its address information. Similarly, it is inherent that at some point the monitored site will also receive address information from the computer at the service center.

Wookey (507) describes in several places the use of authentication information to prevent unauthorized service center personnel from accessing the monitoring software installed at the monitored sites. Column 1, lines 38-43 show that this can be applied in such a way that the authorized service center personnel can log into the customer's system at the monitored site to troubleshoot errors that have been encountered.

With respect to claims 21 and 43, Wookey (507) discloses the method of claim 19 or 41, further comprising the steps of:

in response to the step of authenticating an identity of the user, the processor establishes a packet communications session with a data communications device from which the request to initiate a packet communications session originates. (Col. 4, Lines 12-16)

Wookey (507) discloses that some embodiments of the invention can include the use of the Internet. Those skilled in the computer networking art will recognize that communications over the Internet will require that the data pass through at least one router (data communications device) between its source and its destination. It is inherent that if the data is going through a router, at some point the source computer and destination computer will both have to establish packet communications sessions with the router.

With respect to claims 22, 44, 51, and 55, Wookey (507) discloses the method of claim 21, 43, 50, or 53 wherein the processor is a service processor in the data storage system and the data storage system address information is a pre-configured network address assigned to the service processor associated with the data storage system by a vendor of the data storage system. (Col. 3, Lines 56-59; Col. 4, Lines 12-16)

In column 3, Wookey (507) describes a master monitoring computer at each monitored site, and that this master computer collects the diagnostic information for each monitored computer on the network. This system can be seen in Wookey's figure

1. This is analogous to the service processor of the data storage system, which is depicted in applicant's figure 3 as a computer connected to the data storage system. In regards to the second limitation of the claims, those skilled in the computer arts would know that in Internet communications, every computer has a pre-configured network address assigned to it, known as its IP address.

With respect to claims 23 and 45, Wookey (507) discloses the method of claim 19 or 41 wherein:

the request to initiate a packet communications session is sent from a data communications device interconnected with the computer system; and (Col. 4, Lines 12-17)

wherein the step of providing data storage system address information provides a network address of the processor in the data storage system to the data communications device for receipt by the computer system to allow the computer system to perform packet communications to the data storage system. (Col. 4, Lines 12-17)

Wookey (507) discloses that, "for embodiments in which the internet is used to transmit diagnostic results, the monitored system initiates provision of the diagnostic results without any intervention of the service center." In other words, the monitored system initiates communications over the Internet to the service center. As previously discussed, communications over the Internet necessitate that the data crosses one or more routers between its source and its destination. Thus, when the monitored system

is attempting to establish communications with the service center, it sends a request to a router, and the router forwards the request to the service center. Also as previously mentioned, communications between two computers inherently include the transmission of address information for each computer. In communications over the Internet, this would be the IP address (i.e. the network address) of each computer.

With respect to claims 24 and 46, Wookey (507) discloses the method of claim 19 or 41 the step of establishing a packet communications session with the computer system establishes route information within the data storage system based on the computer system address information to allow the processor o perform packet communications with the computer system. (Col. 4, Lines 12-17)

Though Wookey (507) does not go into great detail about the connection process, those skilled in the art will realize that communications over the Internet include packet routing information to ensure that no data is lost en route.

In regards to claim 57, Wookey (507) discloses the system of claim 56 wherein:

the computer network other than the vendor computer network is a customer computer network; (Figs. 1 and 4)

the data storage system is coupled to the customer computer network; (Figs. 1 and 4)

the connection process is operated by a vendor support engineer in order to provide remote support to the data storage system on the customer computer network; and (Col. 8, Lines 42-45)

the second packet communications session is established from the data communications device to a service processor associated with the data storage system to allow the support engineer operating the connection process to remotely maintain the data storage system using the first and second packet communications sessions. (Col. 8, Lines 42-45)

Wookey (507) discloses in column 8 that, "it is possible to protect each monitor with a unique password so that only authorized administrative personnel can access a given monitor for modification." This implies that those administrative personnel from the service center who are authorized to access a monitor at a customer site are allowed to establish communications via some communications process. Thus, the service personnel are operating a communications process (such as a telnet or ssh connection) to establish communications to the monitored site. Wookey's figures 1 and 4 show a monitored site consisting of a master monitor and a plurality of connected computers. Because a computer will always store some kind of data somehow (whether in a hard drive or in RAM), any computer is a data storage system. Thus, we have personnel from the service center operating a communications process to perform packet communications with a data storage system.

With regards to new claims 59 and 60, Wookey (507) discloses the computer system of claim 18 or 40 wherein a security client is activated on said service processor to block out TCP data packets that have not been encrypted by a predetermined gateway server. (Col. 10, Lines 3-8; It is inherent that if data received at either end of the communications link is not encrypted with the proper dynamic key, that data will be ignored. As previously stated, communications between computers are widely known in the art to be packet-based.)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Virgil Herring whose telephone number is (571) 272-8189. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Virgil Herring
Examiner
Art Unit 2132

VAH

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100